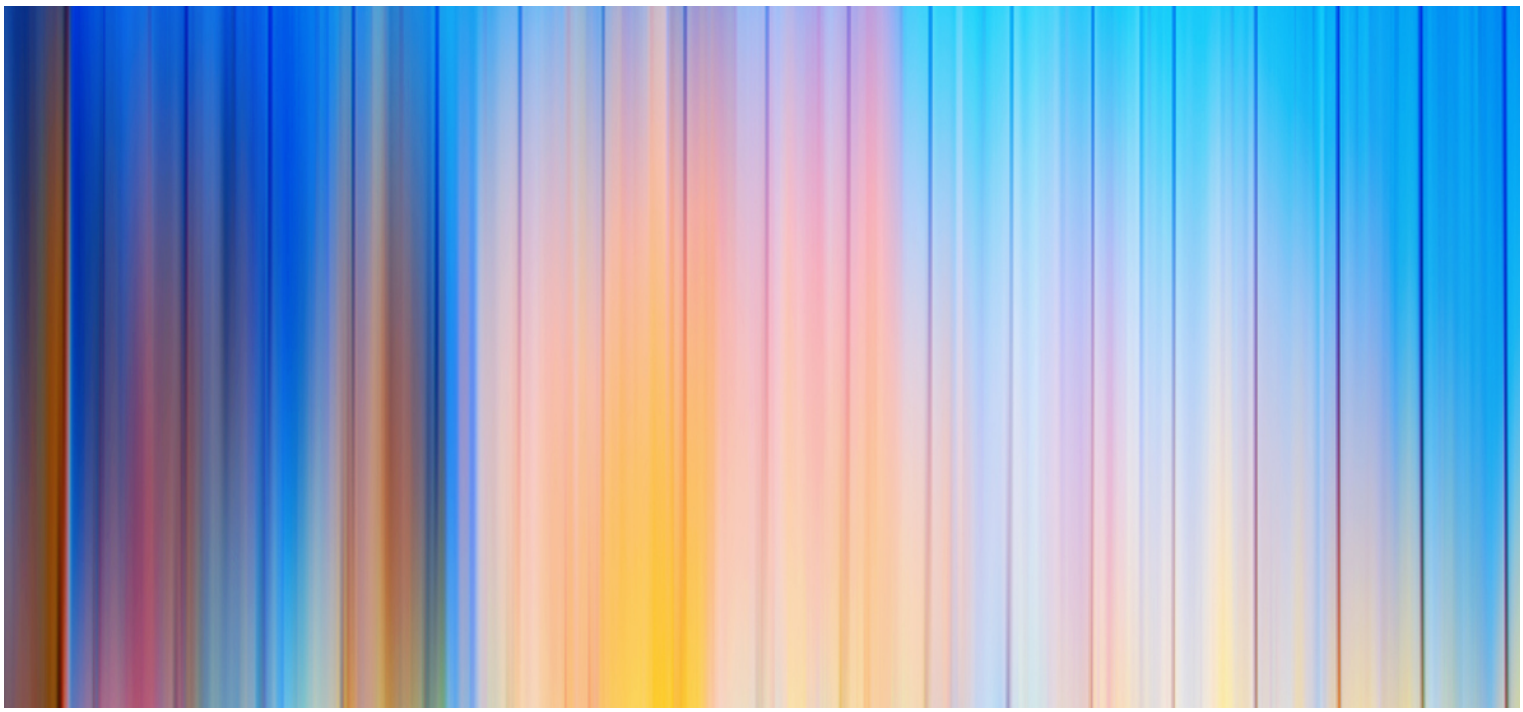
Jun 2021

International: Key takeaways from the new SCCs on international transfers

The European Commission announced, on 4 June 2021, that it had adopted two new sets of Standard Contractual Clauses ('SCCs') on international data transfers which will accentuate the requirements of the General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR'), as well as the Court of Justice of the European Union's judgment in *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (C-311/18)* ('Schrems II'). Odia Kagan, Partner and Chair of GDPR Compliance & International Privacy at Fox Rothschild LLP, provides seven key takeaways from the SCCs, highlighting what companies need to consider moving forward, including third country local laws and supervisory authority designation.



ivanastar / Signature collection / istockphoto.com

1) Bombshell: If your importer is subject to GDPR under Article 3(2), you do not need SCCs

The SCCs are only necessary when the importer is not subject to the GDPR. This also re-ignites the question that could benefit from more clarity regarding the direct applicability of the GDPR to non-EU data processors providing services to EU businesses.

2) The risk-based approach is back!

Parties are required to take into consideration the specific circumstances of the case, including the nature and scope of the data, nature of recipient, and the length of supply chain etc., as well as whether national security requests had been made in the same sector, and even the documented practice experience of the data exporter and data importer.

3) Some attention and respect for third country local laws

The SCCs say that if local law prohibits the deletion or return of the data, the importer shall continue to ensure compliance with the SCCs and only process the data to the extent and for as long as required under local law.

They also say, regarding automated processing, that authorisation under the laws of the country of destination can be an exception to the need for data subject explicit consent for a data importer making a decision based solely on automated processing, provided that such laws lay suitable measures to safeguard the data subject's rights and legitimate interest. In such case, the data importer needs to inform the data subject about the automated decision, the envisaged consequences, and the logic involved.

In the context of the governing law for processor-controller transfers, the clauses allow the governing law which is **NOT** EU Member State law, provided it meets with the requirement: 'These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of (specify).'

4) Emphasis on transparency

Data subjects should be given a copy of the SCCs and be informed, in particular, of the categories of personal data processed, the right to obtain a copy of the SCCs, and any onward transfer.

The obligation of transparency, also on the data importer, is to be carried out, whether directly or through the data exporter, and should include details regarding the onward transfer (recipients or categories of recipients as appropriate with a view to providing meaningful information). The exceptions to this are if the data subject already has this information or if this involves a disproportionate effort for the data importer.

Transparency in the event of a data breach: In case of a data breach resulting in a high risk to the rights and freedoms, the data importer needs to also notify the data subjects and cooperate with the data exporter, unless the data importer implemented measures to significantly reduce the risk or notification would constitute dispropor-

tionate effort. In such case, the data importer should issue a public communication or similar measure to notify the public of the breach.

Transparency in the event of a regulatory investigation: The SCCs contain detailed requirements to notify the data exporter and, where possible, the data subject regarding the legally binding requests for the data or direct access for the data by competent (government) authorities.

For completing the clauses, the instructions are that it must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can be achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

5) Emphasis on security and a shout out to encryption and pseudonymisation

The SCCs align the wording of the security requirements with those of Article 28 of the GDPR, specifically mentioning, 'state of the art, the costs of implementation, the nature scope, context and purpose(s) of processing, and the risks involved in the processing for the data subject' and require a detailed information security exhibit that the parties state 'represents the technical and organisational measures agreed upon by the parties'. The data importer is required to do regular checks to ensure that these measures continue to provide an appropriate level of security. Having recourse to encryption or pseudonymisation, including during transmission, is specifically mentioned.

6) Liability

The SCCs break down some of the practical implementation of liability among multiple parties. In a case where more than one party is responsible for damage caused due to the SCCs, the parties are all jointly and severally liable, but the liable party may claim back from the other party/ies that part of the compensation corresponding to their responsibility for the damage.

7) Acknowledging the unique predicament of the non-EU party regarding supervisory authority designation

The relevant supervisory authority for a non-EU entity party to the SCCs would be of the state where such party has appointed a local representative. If it has not appointed a local representative, then the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these SCCs in relation to the offering of goods or services to them, or whose behavior is monitored, are located as indicated in Annex I.C, shall act as the competent supervisory authority.

Odia Kagan Partner and Chair of GDPR Compliance & International Privacy
okagan@foxrothschild.com
Fox Rothschild LLP, Philadelphia